

# Article 9 of the Second Additional Protocol to the Convention on Cybercrime: Expedited Disclosure of Stored Computer Data in an Emergency

## 1. BACKGROUND

The Council of Europe [Convention on Cybercrime](#) (also known as the Budapest Convention), which was opened for signature in 2001 and entered into force in 2004, was the first international treaty to focus explicitly on cybercrime and electronic evidence. After 20 years, it remains the most significant one in the area. A large number of countries worldwide, including 26 EU Member States<sup>1</sup>, are Parties to the Budapest Convention.



A review of the Budapest Convention is available in the dedicated SIRIUS Quarterly Review [here](#).

In 2003, the Budapest Convention was extended by an [Additional Protocol](#) (First Protocol) covering offences of racist or xenophobic nature.

Following significant developments in the field of information and communication technology which took place since the adoption of the Budapest Convention, on 17 November 2021, after four years of negotiations, the Committee of Ministers of the Council of Europe adopted the [Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence](#) (Second Protocol). The Second Protocol was opened for signature by the Parties to the Budapest Convention in May 2022 and will enter into force after being ratified by at least five Parties<sup>2</sup>.

The Second Protocol is accompanied by an [Explanatory Report](#) intended to assist Parties in its application. The Budapest Convention itself is similarly accompanied by an [Explanatory Report](#) with the same aim.

The Second Protocol is intended to enhance cooperation among the Parties, as well as between the Parties and service providers and other entities, for obtaining disclosure of electronic evidence for the purpose of criminal investigations or proceedings<sup>3</sup>.



More information about the Second Protocol is available in the dedicated SIRIUS Quarterly Review [here](#).

An important provision of the Second Protocol aimed at enhancing cooperation between the Parties is Article 9. Article 9 requires Parties to **adopt the necessary measures** for their **24/7 Network points of contact** established under Article 35 of the Budapest Convention to **transmit and receive requests** from any point of contact in another Party seeking immediate assistance in **obtaining from a service provider in their territory the expedited disclosure of specified, stored computer data in that service provider's possession or control, without a request for mutual assistance**.



More information about the 24/7 Network of points of contact established under Article 35 of the Budapest Convention, including the network's responsibilities under the Budapest Convention, is available in the dedicated SIRIUS Quarterly Review [here](#).

<sup>1</sup> <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treaty-num=185>. All EU Member States, except for Ireland.

<sup>2</sup> Second Protocol, Article 16.

<sup>3</sup> Explanatory Report, para. 25.



The SIRIUS project has received funding from the European Commission's Service for Foreign Policy Instruments (FPI) under contribution agreement No PI/2020/417-500. This document was produced with the financial assistance of the European Union. The views expressed herein can in no way be taken to reflect the official opinion of the European Union.

This document may not necessarily reflect the official position of the Council of Europe or of the Parties to the Budapest Convention on Cybercrime and does not constitute an authoritative interpretation of provisions of this treaty or its protocols.

# Article 9 of the Second Additional Protocol to the Convention on Cybercrime: Expedited Disclosure of Stored Computer Data in an Emergency

Article 9 is **without prejudice to other types of cooperation**, including spontaneous cooperation, **between the Parties**, or **between Parties and service providers**, through other applicable agreements, arrangements, practices or domestic law<sup>4</sup>. Therefore, under the Second Protocol, all of the aforementioned mechanisms remain available to competent authorities that seek data in an emergency. What the Second Protocol does is to set out **two articles which oblige all Parties to provide, at a minimum, specific channels for rapidly expedited cooperation in emergency situations**: Article 9 and Article 10<sup>5</sup>. For more information about Article 10 and a comparison between the two articles, see [section 7](#) and the [annex](#) below.

## 2. SCOPE

### • Types of crimes covered

The measure provided for under Article 9 of the Second Protocol is applicable to **specific criminal investigations or proceedings** relating to:

- Criminal offences established in accordance with Section 1 of the Budapest Convention and other criminal offences committed by means of a computer system;
- The collection of evidence in electronic form of a criminal offence; and
- Between Parties to the First Protocol, criminal offences established pursuant to the First Protocol<sup>6</sup>.

Therefore, the specific criminal investigations and proceedings covered include not only cybercrime, but **any criminal offence involving evidence in electronic form**. This means that the measure provided for under Article 9 of the Second Protocol applies either where a crime is committed by use of a computer system, or where a crime not

committed by use of a computer system (for example a murder) involves electronic evidence<sup>7</sup>.

This is also confirmed in [Guidance Note #13](#)<sup>8</sup>, which states that: “The [Cybercrime Convention Committee (T-CY)] agrees that the procedural law provisions and the principles and measures for international co-operation of the [Budapest Convention] are applicable not only to offences related to computer systems and data but also to the collection of electronic evidence of any criminal offence. This broad scope also applies to the measures of the [Second Protocol].”

### • Definition of “emergency”

“Emergency” is defined in Article 3(2)(c) of the Second Protocol as “a situation in which there is a **significant and imminent risk to the life or safety of any natural person**”. This definition is intended to impose a significantly higher threshold than “urgent circumstances” under Article 25(3) of the Budapest Convention<sup>9</sup>. The definition covers situations in which the **risk is significant and imminent**, meaning that it **does not include** situations in which the **risk to the life or safety of the person has already passed or is insignificant**, or in which **there may be a future risk that is not imminent**<sup>10</sup>.

Emergency situations may involve, for example, **hostage situations** in which there is a **credible risk of imminent loss of life, serious injury or other comparable harm** to the victim; **ongoing sexual abuse of a child**; immediate **post-terrorist attack scenarios** in which authorities seek to determine with whom the attackers communicated in order to **determine if further attacks are imminent**; and **threats to the security of critical infrastructure** in which there is a **significant and imminent risk to the life or safety of a natural person**<sup>11</sup>.

<sup>4</sup> Second Protocol, Article 5(7).

<sup>5</sup> Explanatory Report, para. 150.

<sup>6</sup> Second Protocol, Article 2(1); Budapest Convention, Article 14(2)(a)-(c).

<sup>7</sup> Explanatory Report, para. 33. See also Explanatory Report to the Budapest Convention, paras 141, 243.

<sup>8</sup> Although not binding, Guidance Notes adopted by the T-CY represent the common understanding of the Parties regarding the use of the Budapest Convention and its protocols, see <https://www.coe.int/en/web/cybercrime/guidance-notes>.

<sup>9</sup> Explanatory Report, para. 41.

<sup>10</sup> Explanatory Report, para. 42.

<sup>11</sup> Ibid.

# Article 9 of the Second Additional Protocol to the Convention on Cybercrime: Expedited Disclosure of Stored Computer Data in an Emergency



It is notable that the **definition of an emergency** set out in the **EU Electronic Evidence legislative package** refers specifically to both: (i) an **imminent threat to the life, physical integrity or safety of a person**; and (ii) an **imminent threat to a critical infrastructure**, where the **disruption or destruction** of such critical infrastructure **would result in an imminent threat to the life, physical integrity or safety of a person, including through serious harm to the provision of basic supplies** to the population or to the **exercise of the core functions of the State**<sup>12</sup>.

**Decision-making** with regard to the **existence of an emergency** lies **both with the requesting and the requested Party**. The requesting Party must determine whether an emergency exists before making a request. The requested Party will then assess whether an emergency exists when deciding on the execution of the request.

- **Data covered**

The measure provided for under Article 9 of the Second Protocol can be used for obtaining any specified, stored computer data, that is **subscriber information, traffic data and content data**. The use of this broader term – when compared with other measures provided for under the Second Protocol, such as Article 7 – recognises the **importance of being able to obtain stored content and traffic data**, and not only subscriber information, in **emergency situations**, without requiring the submission of a request for mutual assistance<sup>13</sup>. The term however does not cover any data that has not yet come into existence, such as traffic data or content data related to future communications<sup>14</sup>.



Parties may make a **declaration** that they **will not execute requests** under Article 9 **seeking only the disclosure of subscriber information**<sup>15</sup>. Such a declaration does not however prohibit other Parties from including a request for subscriber information when they are also issuing a request under Article 9 for content and / or traffic data<sup>16</sup>.

A list of all declarations and reservations can be found [here](#).

Article 1(b) of the Budapest Convention defines **computer data** as “any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function”.

The term “**subscriber information**” is defined in Article 18(3) of the Budapest Convention and includes any information held by the administration of a service provider relating to a subscriber to its services (other than traffic data or content data) by means of which can be established:

- The type of communication service used, the technical provisions<sup>17</sup> taken thereto and the period of time during which the person subscribed to the service (Article 18(3)(a));
- The subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, which is available on the basis of the service agreement or arrangement<sup>18</sup> between the subscriber and the service provider (Article 18(3)(b)); or
- Any other information concerning the site or location where the communication equipment is installed, which is available

<sup>12</sup> [Electronic Evidence Regulation](#), Article 3(18).

<sup>13</sup> Explanatory Report, para. 155.

<sup>14</sup> Explanatory Report, para. 155; Explanatory Report to the Budapest Convention, para. 170.

<sup>15</sup> Second Protocol, Article 9(1)(b).

<sup>16</sup> Explanatory Report, para. 157.

<sup>17</sup> The term “technical provisions” includes all measures taken to enable a subscriber to enjoy the communication service, including the reservation of a technical number or address (for

example, telephone number, website address / domain name, e-mail address) and the provision and registration of communication equipment used by the subscriber (for example, telephone devices, call centres, LANs). See Explanatory Report to the Budapest Convention, para. 179.

<sup>18</sup> The reference to a “service agreement or arrangement” includes any kind of relationship on the basis of which a client uses the service provider's services. See Explanatory Report to the Budapest Convention, para. 183.

# Article 9 of the Second Additional Protocol to the Convention on Cybercrime: Expedited Disclosure of Stored Computer Data in an Emergency

on the basis of the service agreement or arrangement (Article 18(3)(c)).



It is notable that the definition of “subscriber information”, as per Article 18(3) of the Budapest Convention, may also include information that under the domestic law of some EU Member States is considered as traffic data.

The term “traffic data” is defined in Article 1(d) of the Budapest Convention and includes any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication’s origin, destination, route, time, date, size, duration, or type of underlying service.

“Content data” is not defined in the Budapest Convention but refers to the content of the communication, i.e. the meaning or purport of the communication, or the message or information being conveyed by the communication (other than traffic data)<sup>19</sup>.

## • Entities covered

The measure provided for in Article 9 of the Second Protocol can be used in order to obtain data from service providers located in the territory of another Party to the Second Protocol. The term “service provider” is broadly defined in Article 1(c) of the Budapest Convention and includes:

- Any public or private entity that provides to users of its service the ability to communicate by means of a computer system; and

- Any other entity that processes or stores computer data on behalf of such communication service or users of such service.

This definition covers both providers of electronic communication services and of internet society services<sup>20</sup>.



It is notable that the definition of “service provider” set out in the EU Electronic Evidence legislative package<sup>21</sup> is broader than the one set out in the Budapest Convention and includes both service providers as defined in Article 1(c) of the Budapest Convention, as well as entities providing domain name registration services, as referred to under Article 6 of the Second Protocol.

Furthermore, the EU Digital Services Act (DSA) applies to providers of “intermediary services”, known as certain information society services which qualify as “mere conduit”, “caching” and “hosting” services<sup>22</sup>. In the field of direct cooperation between authorities and providers of intermediary services active on EU territory, the DSA recognises the potentially overlapping scope of application of the EU Electronic Evidence legislative package. Similarly, providers of intermediary services falling within the scope of the DSA would also fall under the definition of service providers as set out in the Budapest Convention.

## 3. DEFINING THE TOOLBOX

When implemented into the domestic law of the Parties, Article 9 of the Second Protocol will enable a Party, in an **emergency**, to **transmit through its 24/7 Network point of contact** established under Article 35 of the Budapest Convention a **request for data** in the **possession or control** of a service

<sup>19</sup> Explanatory Report to the Budapest Convention, para. 209.

<sup>20</sup> [Guidance Note #10](#), p. 5, footnote 6.

<sup>21</sup> The EU Electronic Evidence legislative package defines a “service provider” as any natural or legal person that provides to its users electronic communication services; internet domain name and IP numbering services such as IP address providers, domain name registries, domain name registrars and domain name related privacy and proxy services; and any other information society service that provides the ability to its users to communicate with each other or makes it possible to store or otherwise process data on behalf of the users to whom the service is provided, where the storage of data is a defining component of the service provided to the user ([Electronic Evidence Regulation](#), Article 3(3); [Electronic Evidence Directive](#), Article 2(1)).

<sup>22</sup> In accordance with Article 3(g) of the DSA, “intermediary service” means one of the following information society services: (i) a “mere conduit” service, consisting of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network; (ii) a “caching” service, consisting of the transmission in a communication network of information provided by a recipient of the service, involving the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients upon their request; (iii) a “hosting” service, consisting of the storage of information provided by, and at the request of, a recipient of the service.

# Article 9 of the Second Additional Protocol to the Convention on Cybercrime: Expedited Disclosure of Stored Computer Data in an Emergency

provider **directly to the 24/7 Network point of contact** in the **territory of the Party in which that service provider is located**, without the need for mutual assistance.

The term “**possession or control**” refers to **physical possession**, as well as to situations where the data is not in the service provider’s physical possession but instead **stored remotely but under the service provider’s control**.

## 4. CONDITIONS AND SAFEGUARDS

### A – OVERALL SYSTEM OF SAFEGUARDS

- **Purpose limitation**

In addition to what is noted above (see section [Scope](#)), requests under Article 9 can only be made in the context of specific criminal investigations or proceeding<sup>23</sup>.

- **Additional safeguards**

Article 9(3) of the Second Protocol, specifying the requirements for requests under Article 9 (see section [Requirements for requests under Article 9](#) below), may assist in applying domestic safeguards<sup>24</sup>. Additionally, Article 9(5) permits a Party to make a declaration that it requires other Parties, following the execution of the request, to submit the request and any supplemental information transmitted in support thereof, in a format and through such channel as specified by it, which may include transmission through mutual assistance channels. The possibility for such additional procedural steps can provide additional safeguards and ensure compliance with domestic law<sup>25</sup>.

### B – ARTICLE 13 OF THE SECOND PROTOCOL: CONDITIONS AND SAFEGUARDS

- **Protection of human rights**

Article 13 of the Second Protocol makes a specific reference to Article 15 of the Budapest Convention and requires Parties to ensure that the powers and procedures established under the Second Protocol – thus including the measure provided for under Article 9 – are subject to an appropriate level of protection for human rights and liberties under their domestic law. These include standards or minimum safeguards arising pursuant to a Party’s obligations under applicable international human rights instruments<sup>26</sup>.

- **Principle of proportionality**

Article 15(1) of the Budapest Convention also requires Parties to apply the principle of proportionality. This will be done in accordance with each Party’s relevant domestic law principles. In the case of European countries, these principles will be derived from the European Convention on Human Rights (ECHR) and related jurisprudence, meaning that the powers of competent authorities must be **proportional to the nature and circumstances of the offence**<sup>27</sup>. Other Parties may apply related domestic law principles, such as principles of **relevance** (i.e. the evidence sought must be relevant to the investigation or prosecution), **limitations on overly broad orders**<sup>28</sup> or **exclude their application in cases concerning minor crimes**<sup>29</sup>.

- **Other conditions and safeguards**

Pursuant to Article 15(2) of the Budapest Convention, applicable conditions and safeguards include, as appropriate, judicial or other independent supervision, grounds justifying the

<sup>23</sup> Second Protocol, Article 2; Explanatory Report, para. 153.

<sup>24</sup> Explanatory Report, para. 219.

<sup>25</sup> Explanatory Report, para. 314.

<sup>26</sup> These instruments include the [1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms](#) (ECHR) and its additional protocols (in respect of European states that are parties to them), other applicable human rights instruments, such as e.g. the [1969 American Convention on Human Rights](#) and the [1981 African Charter on Human Rights and Peoples’ Rights](#) (in respect of

states in other regions of the world which are parties to them) and the [1966 International Covenant on Civil and Political Rights](#) (Explanatory Report to the Budapest Convention, para. 145).

<sup>27</sup> Explanatory Report, para. 97; Explanatory Report to the Budapest Convention, para. 146.

<sup>28</sup> Explanatory Report, para. 97; Explanatory Report to the Budapest Convention, para. 145.

<sup>29</sup> Explanatory Report to the Budapest Convention, paras 146, 174.



# Article 9 of the Second Additional Protocol to the Convention on Cybercrime: Expedited Disclosure of Stored Computer Data in an Emergency

application of the power or procedure and the limitation on the scope or the duration thereof. Other safeguards that must be addressed under domestic law include: the right against self-incrimination, legal privileges, and specificity of individuals or entities subject to the measure<sup>30</sup>.

- **Public interest, sound administration of justice and rights of third parties**

In accordance with Article 15(3) of the Budapest Convention, when implementing the provisions of Article 9, Parties shall first consider the sound administration of justice and other public interests (for example public safety, public health, the interests of victims, respect for private life). To the extent that it is consistent with these interests, consideration shall also be given to the impact of the measure on the rights, responsibilities and legitimate interests of third parties, which may include, for example, protection from liability for disclosure<sup>31</sup>.

## C – ARTICLE 14 OF THE SECOND PROTOCOL: PROTECTION OF PERSONAL DATA

Article 14 of the Second Protocol provides in its paragraphs 2 to 15 a robust system for data protection. This includes safeguards regarding purpose and use of the data; data quality and integrity; sensitive data; retention of data; automated decision-making; security; records and logging; transparency and notice regarding processing, retention periods, data disclosure, access rectification and redress available; right to access and rectification; judicial and non-judicial remedies; and independent oversight<sup>32</sup>. A Party may also suspend the transfer of personal data to another Party based on substantial evidence of systematic or material breach of Article 14<sup>33</sup>.

Pursuant to Article 14(1)(a), each Party shall process personal data that it receives under the Second Protocol in accordance with the specific

safeguards set out in Article 14(2)-(15), with two exceptions:

1. If, at the time of transfer of data, both the transferring Party and the receiving Party are bound by an international agreement establishing a comprehensive framework between those Parties for the protection of personal data, which is applicable to the transfer of personal data for the purpose of the prevention, detection, investigation and prosecution of criminal offences (Article 14(1)(b)). This would include, for example, [Convention 108+](#) and the [EU-US Umbrella Agreement](#)<sup>34</sup>.
2. If the transferring Party and the receiving Party, not bound by an international agreement as described above, nevertheless agree that the transfer of data under the Second Protocol may take place on the basis of other agreements or arrangements between them in lieu of Article 14(2)-(15). For EU Member States, in relation to transfers of personal data to third countries, such an alternative agreement would have to comply with the requirements of EU data protection legislation.

## 5. REQUESTING PARTY

### A – ISSUING AUTHORITIES

Article 9 of the Second Protocol provides flexibility to the requesting Party to determine which of its authorities should initiate the request, such as its competent authorities that are conducting the investigation or its 24/7 Network point of contact, in accordance with domestic law<sup>35</sup>.

<sup>30</sup> Explanatory Report to the Budapest Convention, para. 147.

<sup>31</sup> Explanatory Report to the Budapest Convention, para. 148.

<sup>32</sup> For more information, see Second Protocol, Article 14(2)-(14) and Explanatory Report, paras 227-281.

<sup>33</sup> Second Protocol, Article 14(15).

<sup>34</sup> Explanatory Report, para. 222.

<sup>35</sup> Explanatory Report, para. 156.

# Article 9 of the Second Additional Protocol to the Convention on Cybercrime: Expedited Disclosure of Stored Computer Data in an Emergency

## B – ISSUING PROCEDURE

Article 9 of the Second Protocol similarly provides flexibility to the requesting Party as far as the issuing procedure for Article 9 requests is concerned. This process is outlined in the domestic law of the requesting Party and remains subject to legal safeguards (see also section [Conditions and safeguards](#)).


### REQUIREMENTS FOR REQUESTS UNDER ARTICLE 9

Pursuant to Article 9(3), requests under Article 9 shall specify:

- The **competent authority seeking the data** and the **date** on which the request was issued (Article 9(3)(a));
- A statement that the request is **issued pursuant to the Second Protocol** (Article 9(3)(b)); this will provide assurance that the request is made consistent with the Second Protocol and that any data received as a result of the request will be handled in a manner consistent with the requirements of the Second Protocol. Also, this will **differentiate the request from other emergency disclosure requests** the 24/7 Network point of contact may receive<sup>36</sup>;
- The **name and address of the service provider(s)** in possession or control of the data sought (Article 9(3)(c));
- The **offence(s)** that is / are the subject of the criminal investigation or proceeding and a reference to its / their legal provisions and **applicable penalties** (Article 9(3)(d));
- Sufficient **facts to demonstrate** that there is an **emergency** (as defined in Article 3 of the Second Protocol<sup>37</sup>) and how the **data sought relate to it** (Article 9(3)(e));

- A detailed **description of the data sought** (Article 9(3)(f));
- Any **special procedural instructions** (Article 9(3)(g)); and
- Any **other information that may assist** in obtaining disclosure of the requested data (Article 9(3)(h)); this may include, for example, information which may assist to locate and disclose the stored computer data sought by the requesting Party<sup>38</sup>.

“Special procedural instructions” may include, in particular, **requests for non-disclosure** of the request to subscribers and other third parties<sup>39</sup>.

 In some Parties, confidentiality of the request may be maintained by operation of the law while in other Parties this is not the case. Therefore, in order to avoid the risk of premature disclosure of the investigation, Parties are **encouraged to communicate regarding the need for and any difficulties that may arise in maintaining confidentiality**, including any applicable law, as well as a **service provider’s policies concerning notification**<sup>40</sup>.

“Special procedural instructions” may also include **requests for authentication** of the responsive data. Since such requests can often slow down the key objective of rapid disclosure of the data sought, the authorities of the requested Party should, in consultation with the authorities of the requesting Party, **determine when and in what manner confirmation of authenticity should be provided**<sup>41</sup>.

The requested Party should be able to determine whether an “emergency” within the sense of Article 3(2)(c) of the Second Protocol exists in relation to a request on the basis of the information provided by the requesting Party<sup>42</sup>.

Should the **requested Party require clarification** of the request or **additional information** to act on it, it should **consult with the requesting Party’s 24/7 Network point of contact**<sup>43</sup>.

<sup>36</sup> Explanatory Report, para. 163.

<sup>37</sup> Explanatory Report, para. 164.

<sup>38</sup> Explanatory Report, para. 166.

<sup>39</sup> Explanatory Report, para. 165.

<sup>40</sup> Ibid.

<sup>41</sup> Ibid.

<sup>42</sup> Explanatory Report, para. 154.

<sup>43</sup> Explanatory Report, para. 164.

# Article 9 of the Second Additional Protocol to the Convention on Cybercrime: Expedited Disclosure of Stored Computer Data in an Emergency

Lastly, pursuant to Article 4(1) of the Second Protocol, requests under Article 9 and any accompanying information shall be in a **language acceptable to the requested Party** or be **accompanied by a translation** into such a language.

## TRANSMISSION OF REQUESTS UNDER ARTICLE 9

Article 9 requests are transmitted by the 24/7 Network point of contact of the requesting Party to the 24/7 Network point of contact in the requested Party.

Pursuant to Article 9(4), the requested Party shall accept a request in electronic form. Parties are encouraged to use rapid means of communication to facilitate the transmission of information or data and documents, including transmission of requests<sup>44</sup>. Accordingly, a Party may transmit a request under Article 9 in electronic form, for example by using e-mail, electronic portals or other means. However, there is no requirement that only these formats may be used. A Party may also accept a request transmitted orally (e.g. by phone – a method of communication frequently used by the 24/7 Network<sup>45</sup>) and may require confirmation in electronic form (e.g. via e-mail). Furthermore, appropriate levels of security and authentication may be required.

A Party may make a **declaration** that it requires Parties, **following the execution of the request**, to **submit the request** and any supplemental information transmitted in support thereof **in a format and through such channel as specified** by the requested Party. This may include transmission through mutual assistance channels<sup>46</sup>.

For example, a Party may declare that, in specific circumstances, it will require that a requesting Party submit a subsequent mutual assistance request in order to formally document the emergency request and the prior decision to provide data in response to

such a request. For some Parties such a procedure would be required by their domestic law, whereas other Parties have no such requirements and do not need to avail themselves of this possibility for a declaration<sup>47</sup>.

## 6. REQUESTED PARTY

### A – LEGAL FRAMEWORK FOR EXECUTION

Article 9(2) is designed to **provide flexibility** for Parties in constructing their respective systems for responding to requests under Article 9, considering the differences in domestic law. Parties are however **encouraged** to develop **mechanisms that emphasise speed and efficiency**, are adapted to the exigencies of emergency situations and provide a **broad legal basis for disclosure** of data to other Parties in emergency situations<sup>48</sup>.

Specifically, pursuant to Article 9, Parties are required to adopt the necessary legislative and other measures to ensure that:

- Their **authorities are enabled** under domestic law **to seek and obtain data** requested under Article 9 **from service providers in their territory** and to **respond to such requests** without the requesting Party having to submit a **request for mutual assistance**,<sup>49</sup> and
- **Service providers** in their territory are **permitted to disclose the requested data** to domestic authorities in response to a request under Article 9.

### B – EXECUTION OF THE REQUEST

In accordance with Article 9(6), the requested Party shall **inform the requesting Party of its determination of the request** under Article 9(1) **on a rapidly expedited basis**.

<sup>44</sup> Explanatory Report, para. 167.

<sup>45</sup> Ibid.

<sup>46</sup> Second Protocol, Article 9(5).

<sup>47</sup> Explanatory Report, para. 168.

<sup>48</sup> Explanatory Report, para. 159.

<sup>49</sup> The latter obligation is subject to the possibility to make a declaration in accordance with Article 9(5) that, following the

execution of the request, the requesting Party must submit the request and any supplemental information transmitted in support thereof in a format and through such channel as specified by the requested Party, which may include transmission through mutual assistance channels.



# Article 9 of the Second Additional Protocol to the Convention on Cybercrime: Expedited Disclosure of Stored Computer Data in an Emergency

It is within the discretion of the requested Party to determine:

- Whether the requirements for use of Article 9 have been met;
- Whether another mechanism is more suitable for the purposes of assisting the requesting Party; and
- The appropriate authority to execute a request received by the 24/7 Network point of contact<sup>50</sup>.

While in some Parties, the 24/7 Network point of contact may already have the requisite authority to execute the request itself, other Parties require that their point of contact forward the request to another authority or authorities to seek disclosure of data from the service provider concerned. In some Parties, this may require obtaining a judicial order. The requested Party also has discretion to determine the channel for transmitting the responsive data to the requesting Party, be it through the 24/7 Network point of contact or through another authority<sup>51</sup>.

Article 9 refers to “requests” and **does not compel** requested Parties **to provide the requested data** to the requesting Party; therefore, there **may be situations** where the **requested Party will not execute the request**. For example, the requested Party may determine that, in a particular case, emergency mutual assistance under Article 10 or another means of cooperation would be most appropriate<sup>52</sup>.

If applicable, the requested Party shall also **specify any conditions** under which it would provide the data and **any other forms of cooperation that may be available**<sup>53</sup>. For example, the requested Party may provide the data within a matter of hours, but should the competent authority seeking the data wish to use it in court, it may need to follow-up with a formal mutual assistance request.

The requested Party that **supplies information or material subject to a condition** may also require

the requesting Party to **explain** in relation to that condition **the use made of such information or material**<sup>54</sup>, in order to ascertain whether such condition has been complied with<sup>55</sup>. It is, however, understood, that the requesting Party may not call for an overly burdensome accounting<sup>56</sup>.

If a requesting Party cannot comply with a condition imposed by the requested Party under Article 9(6), it shall **promptly inform the requested Party**. The requested Party shall then **determine whether the information or material should nevertheless be provided**. By contrast, if the requesting Party accepts the condition, it shall be **bound by it**<sup>57</sup>.

## 7. COMPARISON BETWEEN ARTICLE 9 AND ARTICLE 10 OF THE SECOND PROTOCOL

While Article 9 of the Second Protocol is intended to facilitate **access to data** in an **emergency without** resorting to **mutual assistance**, Article 10 is intended to provide a **rapidly expedited procedure for mutual assistance** requests made in **emergency situations**. It is up to the Parties, based on their accumulated experience and the specific legal and factual circumstances at hand, to decide which is the best channel to use in a particular case<sup>58</sup>. Article 9, for example, could constitute a faster way for seeking content data while Article 10 could be a natural choice when a more formal way of cooperation would be required or when there would be a need to request additional forms of cooperation and not just electronic evidence.

See the [annex](#) for a comparison matrix between Article 9 and Article 10 of the Second Protocol.



More information about Article 10 of the Second Protocol is available in the dedicated SIRIUS Quarterly Review available on the [SIRIUS subpage](#) on Eurojust’s website.

<sup>50</sup> Explanatory Report, para. 160.

<sup>51</sup> Ibid.

<sup>52</sup> Explanatory Report, para. 169.

<sup>53</sup> Second Protocol, Article 9(6).

<sup>54</sup> Second Protocol, Article 9(7)(b).

<sup>55</sup> Explanatory Report, para. 170.

<sup>56</sup> Ibid, referring, by analogy, to Explanatory Report to the Budapest Convention, paras 279-280.

<sup>57</sup> Second Protocol, Article 9(7)(a).

<sup>58</sup> Explanatory Report, para. 152.

## Article 9 of the Second Additional Protocol to the Convention on Cybercrime: Expedited Disclosure of Stored Computer Data in an Emergency



### ANNEX: COMPARISON MATRIX BETWEEN ARTICLE 9 AND ARTICLE 10 OF THE SECOND PROTOCOL

Legal provision	Article 9	Article 10
<b>Purpose</b>	Facilitating access to data in an emergency	Providing a rapidly expedited procedure for mutual assistance
<b>Request process</b>	No formal mutual assistance request needed	Requires a formal mutual assistance request
<b>Time efficiency</b>	Generally faster	May be faster with close working relationships
<b>Information exchange</b>	Real-time exchange	More formal and written communication
<b>Scope of cooperation</b>	Obtaining stored computer data (subscriber information, traffic data, content data)	Can request additional forms of cooperation
<b>Evidence authentication</b>	May be more challenging	May be easier